



①9 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENT- UND  
MARKENAMT

⑫ **Offenlegungsschrift**  
⑩ **DE 199 37 529 A 1**

⑤ Int. Cl.<sup>7</sup>:  
**G 06 K 19/073**  
G 07 F 7/10

②1 Aktenzeichen: 199 37 529.1  
②2 Anmeldetag: 9. 8. 1999  
④3 Offenlegungstag: 1. 3. 2001

DE 199 37 529 A 1

⑦1 Anmelder:  
Giesecke & Devrient GmbH, 81677 München, DE

⑦2 Erfinder:  
Böhler, Jürgen, 81827 München, DE

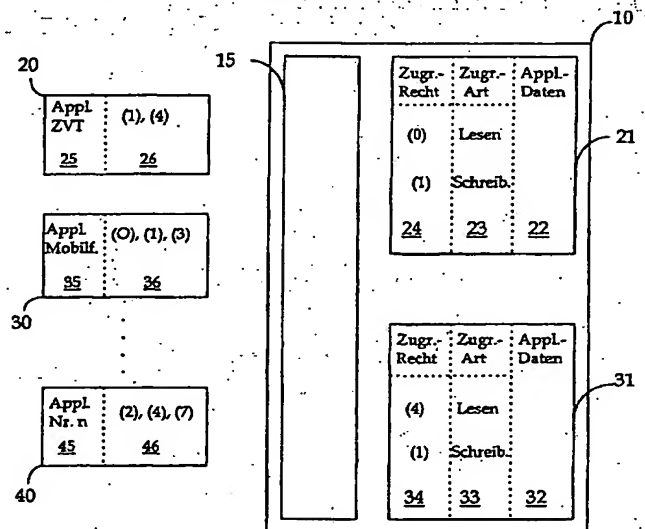
⑤5 Entgegenhaltungen:  
DE 3 784 82 4T2  
BEUTELSPACHER, KERSTEN, PFAU: Chipkarten  
als Sicherheitswerkzeug, Springer-Verlag,  
Berlin 1991, ISBN 3-540-54140-3, S. 76-85;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Tragbarer Datenträger und Verfahren zur Nutzung in einer Mehrzahl von Anwendungen

⑤7 Vorgeschlagen wird ein tragbarer Datenträger zur Nutzung in einer Mehrzahl von Anwendungen mit einer Speichereinrichtung, worin sich mindestens ein Datenfeld (21, 31) befindet, auf das von in einer Kartenanwendungsvorrichtung realisierten Applikationen auf mehrere Arten zugegriffen werden kann, sowie einer Zugriffssteuereinrichtung (15) zur Kontrolle der Zugriffe auf die Datenfelder (21, 31). Jedem Datenfeld (21, 31) ist eine Tabelle (23, 24, 33, 34) zugeordnet, die allen möglichen Zugriffsarten jeweils ein Zugriffsrecht zuordnet. Entsprechend ist jeder Applikation mindestens ein Zugriffsrecht zugeordnet. Im Falle einer Zugriffsabsicht prüft die Zugriffssteuereinrichtung (15), ob die den Zugriff beabsichtigende Applikation über das für den beabsichtigten Zugriff erforderliche Zugriffsrecht verfügt.



DE 199 37 529 A 1

## Beschreibung

Die Erfindung geht aus von einem tragbaren Datenträger nach der Gattung des Hauptanspruchs.

Ein solcher ist in der Gestalt einer Chipkarte beispielsweise aus EP 262 025 B1 bekannt. Die Schrift offenbart ein Zugriffssystem zur Gewährung des Zugriffs auf Datenfelder einer IC-Karte für mehrfache Dienste. Jeder Dienst bzw. jede Anwendung besitzt einen spezifischen Authentisierungscode. Auf der IC-Karte ist desweiteren jedem Datenfeld ein Zugriffsinformationsspeicher zugeordnet, der jedem möglichen Authentisierungscode spezielle Zugriffsrechte für das jeweilige Datenfeld zuordnet. Das System arbeitet so, daß jeder Dienst nur auf vorbestimmte Art auf definierte Datenfelder zugreifen kann. Es erfordert allerdings eine unter Umständen aufwendige Pflege der Zugriffsinformationsspeicher. Soll etwa ein neuer Dienst bzw. eine neue Anwendung Zugriff auf bereits vorhandene haben, müssen die Zugriffsinformationsspeicher aller betroffenen Datenfelder geändert werden.

Der Erfindung liegt die Aufgabe zugrunde, einen tragbaren Datenträger für Mehrfachanwendungen sowie ein Verfahren zur Regelung der Zugriffsmöglichkeiten bezüglich der Mehrfachanwendungen anzugeben, die die Vornahme von Änderungen in der Anwendungsstruktur vereinfachen.

Diese Aufgabe wird gelöst durch einen tragbaren Datenträger mit den Merkmalen des Anspruchs 1 sowie ein Verfahren mit den Merkmalen des unabhängigen Anspruchs 3. Der erfindungsgemäße Datenträger hat den Vorteil, daß er leicht ausbaufähig ist. Ohne weiteres lassen sich neue Anwendungen als Applikationen implementieren und die zugehörigen Datenfelder auf den Datenträger bringen. Ein Eingriff in bereits vorhandene Applikationen bzw. die zugehörigen Datenfelder ist nicht erforderlich. Auch eine genaue Kenntnis der bereits vorhandenen Applikationen bzw. Datenfelder ist nicht notwendig. Dennoch können vorhandene Datenfelder ohne Gefährdung der Sicherheit für unterschiedliche Anwendungen nutzbar gemacht werden. Insbesondere werden unberechtigte Übergriffe zwischen verschiedenen auf einem Datenträger vorhandenen Applikationen verhindert. Alle Änderungen in der Anwendungsstruktur können dabei jederzeit vorgenommen werden. Ein Vorteil des aus Anspruch 3 entnehmbaren Verfahrens besteht auch darin, daß es wenig Speicherplatz benötigt.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend unter Bezugnahme auf die Zeichnung näher erläutert.

Es zeigen:

Fig. 1 die Struktur eines Datenträgersystems,

Fig. 2 die Anordnung von Zugriffsinformationen in Anwendungsstrukturen und Datenträger,

Fig. 3 den Ablauf eines Zugriffs einer Applikation auf ein Datenfeld.

In Fig. 1 bezeichnet die Bezugszahl 10 einen zur Nutzung in einer Mehrzahl von Anwendungen ausgebildeten Datenträger, der in Form einer Chipkarte ausgebildet ist. Auf ihr befinden sich eine zentrale Prozessoreinheit 11 zur Ausführung von Programmcode, welcher jeweils eine Chipkartenfunktion realisiert, eine Speichereinrichtung 12, worin der von der zentralen Prozessoreinheit 11 auszuführende Programmcode abgelegt ist, sowie eine Schnittstelle 14 zum Austausch von Daten mit verschiedenen Anwendungen realisierenden Kartenanwendungsvorrichtungen 20, 30. Als Beispiele für mögliche Kartenanwendungsvorrichtungen sind in Fig. 1 ein Zahlungsverkehrsterminal 20 sowie ein Mobilfunkgerät 30 angedeutet. Jede Kartenanwendungsvorrichtung 20, 30 dient zur Realisierung wenigstens einer Applikation, zu der auf der Chipkarte 10 jeweils ein Applikations-Datencode korrespondiert, welcher als separates Datenfeld

21, 31 im Speicher 12 ausgebildet ist. Eine über eine Kartenanwendungsvorrichtung 20, 30 realisierte Applikation kann nur auf Datenfelder 21, 31 zugreifen, für die sie eine Zugriffsberechtigung besitzt.

Die Struktur des eingesetzten Zugriffsberechtigungssystems ist in Fig. 2 veranschaulicht. Die Kartenanwendungsvorrichtungen 20, 30 sind jetzt durch Blöcke repräsentiert. Jede Kartenanwendungsvorrichtung, mithin jeder Block 20, 30, ist mit – nicht weiter gezeigten – signaltechnischen Mitteln ausgestattet, die es ermöglichen, einen Zugriff auf ein Datenfeld 21, 31 im Speicher 12 der Chipkarte 10 einzuleiten. Parallel zu den schon beispielhaft benannten Anwendungen Zahlungsverkehr und Mobilfunk können weitere gleichartige oder verschiedene Kartenanwendungsvorrichtungen angeordnet sein, was durch Block 40 angedeutet ist. Der in jeder Kartenanwendungsvorrichtung 20, 30 vorhandene Datencode umfaßt jeweils einen Teil 35, 45 mit dem Code einer eine Kartenanwendung umsetzenden Applikation, etwa Informationen zu einem Konto im Zusammenhang mit einer Zahlungsverkehrstransaktion oder Authentifizierungsinformationen für ein Mobilfunkgerät; daneben umfaßt er jeweils einen Abschnitt 36, 46 mit Daten, die für die auf der Kartenanwendungsvorrichtung 20, 30 vorhandenen Anwendungsapplikationen einen vorrichtungsseitigen Zugriffsstatus festlegen. Die Zugriffsstatusdaten definieren dabei Zugriffsrechte und Zugriffsarten wie beispielsweise Lesen, Schreiben, usw., die angeben, auf welche Art die Applikationen jeweils auf ein Datenfeld 21, 31 in der Chipkarte 10 zugreifen können. Jede Applikation kann über ein oder mehrere Zugriffsrechte verfügen. In einfacher Weise kann dabei, wie in Fig. 2 angedeutet, jedes Zugriffsrecht durch eine Ziffer symbolisiert sein. Im Beispiel der Fig. 2 sind der Applikation 20 Zugriffsrechte (1) und (4), der Applikation 30 Zugriffsrechte (0), (1) und (3), der Applikation 40 Zugriffsrechte (2), (4) und (7) zugeordnet.

Repräsentativ für die Chipkarte 10 stehen in Fig. 2 eine Zugriffssteuereinrichtung 15 sowie den Kartenanwendungsvorrichtungen 20, 30 zugeordnete Datenfelder 21, 31. Die Zugriffssteuereinrichtung 15 ist dabei eine Teilfunktion der nicht weiter gezeigten zentralen Prozessoreinheit 11, die Datenfelder 21, 31 sind in der Speichereinrichtung 12 realisiert. In Analogie zu den Kartenanwendungsvorrichtungen 20, 30, 40 können in der Speichereinrichtung 12 neben den beiden angedeuteten weiteren Datenfelder vorhanden sein, die der Übersichtlichkeit wegen nicht dargestellt sind.

Korrespondierend zu den Zugriffsrechten der Kartenanwendungsvorrichtungen 20, 30 weisen die auf der Karte angelegten Datenfelder 21, 31 neben den Nutzdaten 22, 32 jeweils noch weitere Abschnitte mit Zugriffsinformationen, 23, 24, 33, 34 auf. Ein erster Abschnitt 23, 33 enthält dabei die in Bezug auf das zugrundeliegende Datenfeld 21, 31 überhaupt möglichen Zugriffsarten, z. B. Schreiben, Lesen usw. Ein zweiter Abschnitt 24, 34 ordnet jeder im ersten Abschnitt enthaltenen Zugriffsart jeweils ein zur Ausführung der Zugriffsart benötigtes Zugriffsrecht zu. Die Angabe des Zugriffsrechtes erfolgt dabei übereinstimmend mit der in den Kartenanwendungsvorrichtungen verwendeten Darstellung. Sie kann in einfacher Weise insbesondere in der Zuordnung von Ziffern zu bestimmten Zugriffsarten bestehen.

Den Zugriff einer Anwendungsapplikation auf ein Datenfeld 21, 31 vermittelt die Zugriffssteuereinrichtung 15. Fig. 3 veranschaulicht die dabei durchgeführten, grundsätzlichen Verfahrensschritte am Beispiel einer Mobilfunksituation, in der eine über die Luftschnittstelle wirkende Applikation auf den Kurzwahlnummernspeicher einer in einem Mobilfunkgerät eingesetzten Chipkarte zugreift, um etwa die Kurzwahlnummernliste zu aktualisieren, Schritt 100. Erkennt die Zugriffssteuereinrichtung 15, nach einer entsprechenden In-

italisierung, daß eine Applikation – im Beispiel in Gestalt einer über die Luftschnittstelle übertragenen Aktualisierungsapplikation – einen Zugriff auf ein kartenseitiges Datenfeld 21, 31 beabsichtigt, bestimmt sie zunächst den Typ des beabsichtigten Zugriffs. Steht fest, auf welche Art der Zugriff – im Beispiel: Zunächst Lesen – erfolgen und auf welches Datenfeld 21, 31 – im Beispiel: den Kurzwahlnummernspeicher – zugegriffen werden soll, ermittelt die Zugriffssteuereinrichtung 15 aus dem Datenfeld 21, 31 mit Hilfe der jeweils entsprechenden Tabelle 23, 24, 33, 34, welches Zugriffsrecht der beabsichtigte Zugriff kartenseitig erfordert, Schritt 102 – die Zugriffsart Lesen erfordert beispielsweise das Zugriffsrecht mit der Nummer (4). Hierauf ermittelt die Zugriffssteuereinrichtung 15, Schritt 104, ob der der Applikation vorrichtungsseitig zugeordnete Zugriffsstatus das benötigte Zugriffsrecht umfaßt – im Beispiel: verfügt die Applikation vorrichtungsseitig zumindest über das Zugriffsrecht Nummer (4) für Lesen. Enthält der für die Applikation ermittelte Zugriffsstatus das benötigte Zugriffsrecht, wird der von der Applikation beabsichtigte Zugriff erlaubt, Schritt 106. Enthält der ermittelte Zugriffsstatus der Applikation das benötigte Zugriffsrecht nicht oder nicht vollständig, wird der beabsichtigte Zugriff nicht verweigert, Schritt 108.

Das vorbeschriebene Zugriffs-konzept ist sowohl karten-extern durch Hinzunahme weiterer Kartenanwendungsvorrichtungen wie kartenintern durch Hinzufügung weiterer Datenfelder erweiterbar. Neu auf eine Chipkarte gebrachten Datenfeldern fügt zweckmäßig die Zugriffssteuereinrichtung 15 beim Laden jeweils eine Zugriffsinformationstabelle 23, 24, 33, 34 zu. Da die Zugriffsstatusdaten nicht datenfeldspezifisch sind, können Anwendungsapplikationen die aufgrund ihres vorrichtungsseitigen Zugriffsstatus möglichen Zugriffsarten bezüglich aller datenträgerseitigen Datenfelder 21, 31 vornehmen, die für einen Zugriff ein in dem Zugriffsstatus enthaltenes Zugriffsrecht erfordern.

#### Patentansprüche

1. Tragbarer Datenträger zur Nutzung in einer Mehrzahl von Anwendungen mit einer Speichereinrichtung, worin sich mindestens ein Datenfeld befindet, auf das von wenigstens einer, in einer Kartenanwendungsvorrichtung realisierten Anwendungsapplikation auf mehrere Arten zugegriffen werden kann, sowie einer Zugriffssteuereinrichtung, die Applikationen, welche einen Zugriff auf ein Datenfeld beabsichtigen, auf ihre Berechtigung dazu prüft, **dadurch gekennzeichnet**, daß dem Datenfeld (21, 31) eine Tabelle (23, 24, 33, 34) zugeordnet ist, die den möglichen Zugriffsarten jeweils ein Zugriffsrecht zuordnet, und die Zugriffssteuereinrichtung (15) aufweist:
  - Mittel, um die Art eines von einer Applikation beabsichtigten Zugriffs auf ein Datenfeld (21, 31) festzustellen,
  - Mittel, um aus der Tabelle (23, 24, 33, 34) des Datenfeldes (20, 21), auf das ein Zugriff beabsichtigt ist, ein der festgestellten Zugriffsart zugeordnetes Zugriffsrecht zu entnehmen,
  - sowie Mittel, um festzustellen, ob eine Applikation, die einen Zugriff beabsichtigt, über ein bestimmtes Zugriffsrecht verfügt.
2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß zumindest den Zugriffsarten Lesen, Schreiben, Ausblenden, Wiederherstellen jeweils ein eigenes Zugriffsrecht zugeordnet ist.
3. Verfahren zur Regelung des Zugriffs einer in einer

Kartenanwendungsvorrichtung realisierten Applikation auf ein Datenfeld eines für eine Mehrzahl von Anwendungen nutzbaren tragbaren Datenträgers, gekennzeichnet durch folgende Schritte:

- Zuordnen eines Zugriffsrechtes zu jeder möglichen Zugriffsart für jedes Datenfeld, und
  - im Falle einer Zugriffsabsicht:
  - Feststellen der Art des beabsichtigten Zugriffs,
  - Bestimmen des der festgestellten Zugriffsart für das betroffene Datenfeld (21, 31) zugeordneten Zugriffsrechtes,
  - Feststellen, ob die den Zugriff beabsichtigende Applikation über ein bestimmtes Zugriffsrecht verfügt.
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Zuordnung eines Zugriffsrechtes zu einer Zugriffsart beim Laden eines Datenfeldes (21, 31) auf den Datenträger (10) erfolgt.
  5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Zuordnung von Zugriffsrechten zu einer Applikation und zu einem Datenfeld (21, 31) eines Datenträgers (10) unabhängig voneinander erfolgen.

---

Hierzu 2 Seite(n) Zeichnungen

---

- Leerseite -

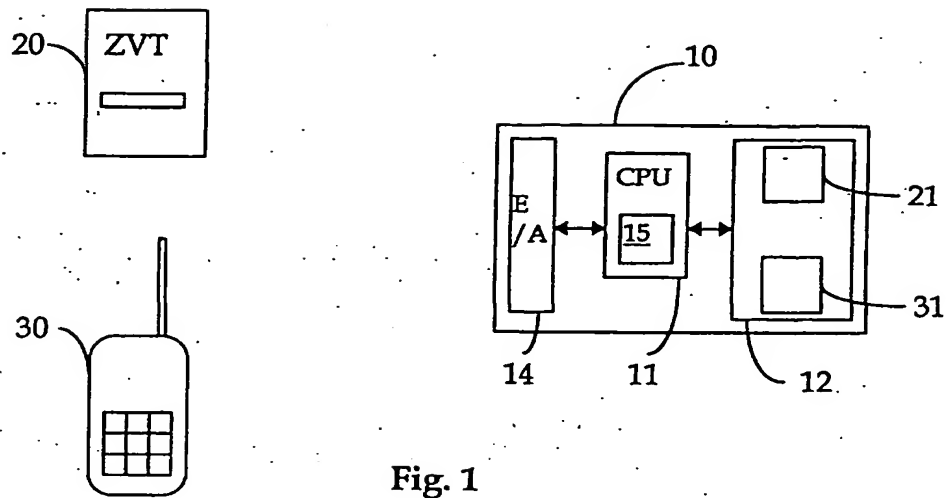


Fig. 1

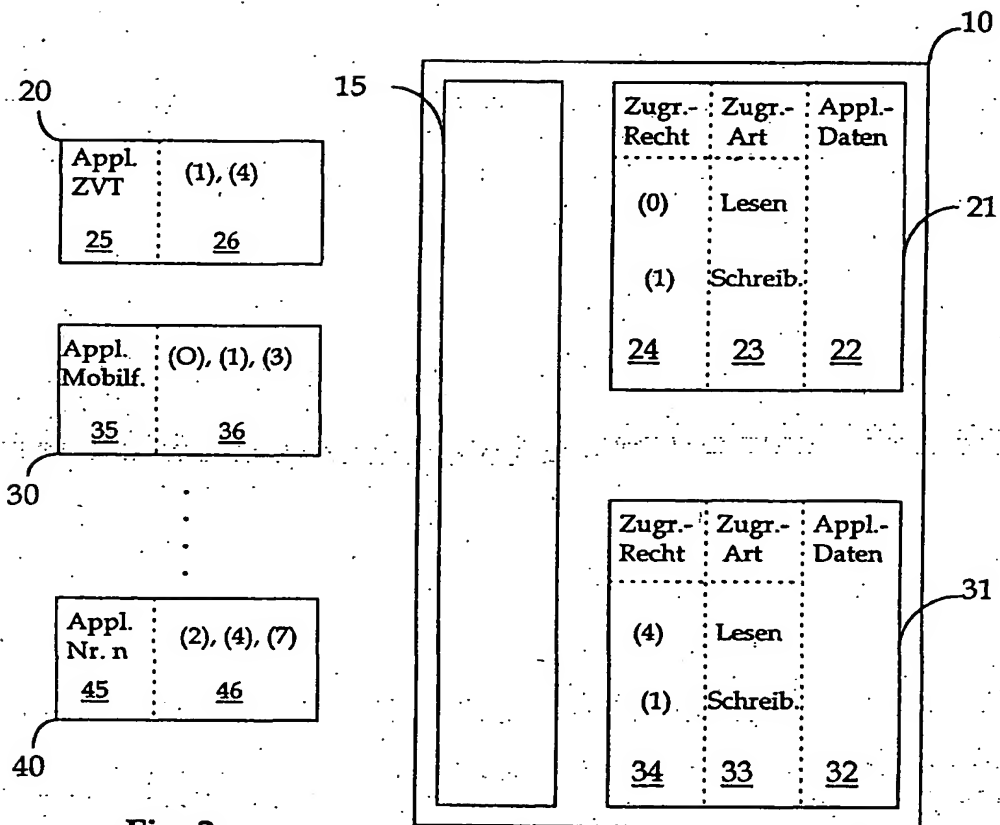


Fig. 2

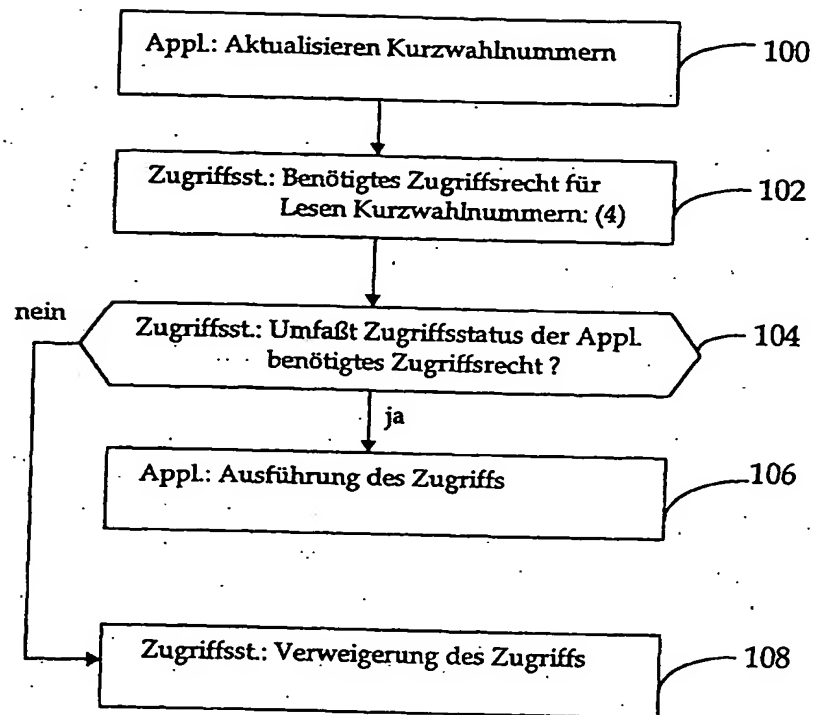


Fig. 3